COMMITTEE ON
SCIENCE, SPACE, AND TECHNOLOGY
REPUBLICANS Frank Lucas, Ranking Member

Opening Statement of Subcommittee Ranking Member Brian Babin

Subcommittee on Space Hearing
“Cybersecurity at NASA: Ongoing Challenges and Emerging Issues for Increased Telework During COVID-19”

September 18th, 2020

NASA is one of the best-known organizations in the world. Its successes with the Mercury, Gemini, Apollo, Shuttle, and International Space Station programs – along with its breathtaking scientific discoveries and jaw-dropping robotic probes – attract worldwide attention. Unfortunately, that attention comes with challenges. The technologies that NASA develops are also sought-after by criminal entities, unscrupulous foreign governments, and destructive vandals. Because many of these technologies have both civil and military applications, these challenges are particularly grave.

This is a topic that this Committee has focused on for decades. One of our witnesses, NASA Inspector General Martin, testified before the Investigations and Oversight Subcommittee almost ten years ago on information security. At that hearing, he testified that an unencrypted laptop was stolen from NASA that “resulted in the loss of the algorithms” used to control the space station, as well as personally identifiable information and intellectual property.

Similarly, the U.S. China Economic and Security Review Commission noted in its 2011 report to Congress that the Terra and Landsat-7 satellites “experienced at least two separate instances of interference apparently consistent with cyber activities against their command and control systems.” More recently, the NASA Office of the Inspector General issued its yearly FISMA report in July, which found that “…information systems throughout the Agency face an unnecessarily high level of risk that threatens the confidentiality, integrity, and availability of NASA’s information.” The report concluded that “…it is imperative the Agency continue its efforts to strengthen its risk management and governance practices to safeguard its data from cybersecurity threats.” And last month, the NASA Office of the Inspector General issued another report on NASA's use of non-agency IT Devices that found that "NASA is not adequately securing its networks from unauthorized access by IT devices." The NASA Inspector General is currently tracking 25 open recommendations for the Office of the Chief Information Officer. These do not include IT and cybersecurity recommendations to Mission Directorates or other organizations in the NASA enterprise.

While this may seem startling, there are specific reasons that many of the recommendations remain open. For instance, agency-wide guidelines and best practices are often general rules and principles that are not optimized to specific agencies unique capabilities, expertise, and challenges. For example, NASA is the world leader in designing, building, operating, and communicating with spacecraft. This expertise resides within the Mission Directorates and at the Centers who have cultivated this skillset over decades. In some instances, they actually developed the software, information systems, and underlying technologies that industry and the rest of the government adopted and embraced.

In even more extreme circumstances, they continue to use one-off operating systems that, while perhaps not compliant with OMB-derived government-wide guidance, are arguably more secure because of their uniqueness and obscurity. Efforts to bring these systems and technologies into compliance with one-size-fits-all, cookie-cutter approaches developed for commercial and enterprise systems could actually introduce more risk. This isn't to excuse NASA's cybersecurity shortcomings as identified by the IG and GAO over the years. Lost laptops, unsecured devices, unauthorized access to systems, and lapsed ATOs (or "Authorization to Operate"), and poor inventory management are all cause for concern.

Which brings us to the situation NASA currently faces. The COVID-19 challenge requires most of NASA's employees and contractors to work remotely. While NASA has embraced teleworking for years, the expansion of this practice introduces a larger target and more vulnerabilities for malicious actors to exploit.

In addition to teleworking challenges, I am also interested in understanding what level of insight NASA has on contractor cybersecurity as NASA moves more to public-private partnerships. Finally, it's worth noting that President Trump recently issued Space Policy Directive 5 focused on cybersecurity principles for space systems. While it is not focused on COVID specifically, it is particularly timely given today's hearing and demonstrates the Administration's forward-looking leadership on the topic.

I look forward to hearing more about these critical issues, what NASA plans to do to mitigate them, as well as what Congress and the Administration can do to help.

Thank you, I yield back.